**IT Applications, Unit 4**

**Security and ethical considerations, Ch 8, p 285**

Security Equipment

**Security hardware**

1. What is meant by data integrity?

Data integrity is the assurance that data is accurate and reliable, and is available in a timely manner.

1. Biometrics
   1. Describe biometric security.

In biometric security the body or physical attributes of the user are used for their secure information and authentication.

* 1. Why does it appeal to security managers?

It appeals to secure managers because it is nearly impossible to copy or steal a person’s biometric characteristics.

* 1. List the common biometric devices.
* Voice recognition
* Fingerprint recognition
* Hand geometry
* Signature verification
* Facial recognition
* Iris recognition
  1. What are the concerns of biometric technology?

The concerns Cost and intrusive

1. Swipe cards
   1. Describe the nature of a swipe card.

They are usually a business-card sized plastic card with a magnetic strip on one side and user details stamped or printed on the other side.

* 1. What is a limitation of the swipe card?

The card can be easily damaged by magnetic fields and if stolen, they offer little protection from a thief with a swipe-card reader that can capture the data on it.

1. Smart cards

It looks simular to swipe cards, except that it has a microchip embedded in it to store and manipulate data.

1. Security tokens

When dealing with sensitive information, a small device about the size of a key ring may be used to constantly changing authorisation codes.

1. Mobile phone secure code
   1. How does this level of authentication work?

Authentication occurs when a security code is sent to the account holders mobile phone to authenticate a transaction before it actually occurs.

**Power protection**

Outline the characteristics of the following:

1. Surge protector

It protects electricity equipment against overvoltage caused by power surges.

1. Uninterruptible power supply, (UPS)

It protects against power spikes and provides power when there is a loss of power.

**Strategies for avoiding system failure, p 288**

1. What is meant by redundancy?

In this context, redundancy means no single part of the system is critical to its overall operation.

1. What is meant be a fault-tolerant server?

A fault-tolerant server will continue to work even when a piece of hardware has failed.

1. Redundancy through multiple hard drives or fault-tolerant equipment
   1. Describe how this redundancy works.

If one part fails, the others can take over its job and keep the system running until the part is replaced.

* 1. What is meant by RAID technology

In a RAID-protected system, fragments of data are spread over several hard drives, so that if one hard drive fails, the others can piece together the missing data.

1. Redundancy through mirrored servers or machines
   1. Why is the RAID solution preferable to this solution?

**Backup Media**

1. There are a range of options for backup media, what 3 factors should be considered when deciding on which backup media to use?

Three categories of backup media:

* Magnetic media
* Optical drives
* Solid-state drives

List the characteristics of the following backup media:

**Magnetic media**

1. hard disk drive

An affordable option and useful if you have many files.

1. Magnetic tapes

Cheap but slow to save and restore files.

**Optical media**

1. Compact disc

Removable storage can be used once or multiple time

1. DVD

Can store up to 17GB

1. Blu-ray

Can store 50GB of data

**Solid-state drives**

1. USB storage devices

No moving parts, portable and can hold 256GB of data.

**Online backups**

1. Why do organisations use this form of backup?

Organisation use online backup so they can work efficiently and effectively as possible.

1. Describe an enterprise storage system.

It is offsite storage by a provider over the internet.

**Surveillance technology, p 292**

Describe the nature of the following items of surveillance equipment used in offices:

1. Packet sniffers

They are diagnostic tools that monitor the contents of packets of data being sent across networks.

1. Desktop monitoring programs

Works by intercepting every single action preformed on a computer.

1. Log files

Similarly, our own web browsers store accessed webpages and images in cache and keep a local file of our browsing history.

1. Closed-circuit television, (CCTV)

Allows employers access to workplace computers.

1. Telephones
2. Audit trails

**Physical security devices:** List the options for physically securing your data